КРИМІНАЛЬНА КІБЕРПРОТИПРАВНІСТЬ-ЧИННИК ЗАГРОЗ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Юлія Володимирівна КЛЕТЬОНКІНА,

студентка Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Науковий керівник: *к.ю.н., професор Шинкаренко І. Р.*

У чинній Доктрині інформаційної безпеки України визначено, що до важливих інтересів особи та життєво важливих інтересів суспільства і держави. відноситься забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів. Окрім того до таких інтересів відноситься всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації; розвиток та захист національної інформаційної інфраструктури; формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів; безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір; забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України та ін [1].

Таким чином проблема кіберзлочинності є дуже актуальною та важливою в наш час. Означене обумовлено бурхливим розвитком інформаційних технологій в Україні і як наслідок розвитком злочинності у цій сфері. З'явився новий феномен кіберзлочинність.

Кіберзлочинність входить до трійки головних небезпек в усьому світі. Найбільше від цього виду злочинності страждають розвинені країни . З розвитком речей , які мають доступ до Інтернету, під удар частіше потрапляють банківські онлайн-сервери , електромережі , бортові комп'ютери автомобілів , літаків , а як наслідок – люди [2].

Згідно з дослідженням Асоціації виробників програмного забезпечення (BSA), рівень піратства в Україні становив 84%. За оцінками Міжнародного альянсу інтелектуальної власності (IIPA), Україну визнано «піратом №1» у світі [3].

Щорічно зростає кількість кримінальних правопорушень зв'язаних з використанням електронно обчислювальних пристроїв та інформаційних систем. Так у 2017 році в Україні відбулася масштабна атака вірусом Petya: були уражені енергетичні компанії, українські банки, аеропорт «Бориспіль», аеропорт Харкова, Чорнобильська АЕС, урядові сайти, київський метрополітен тощо.

Фактично була створена глобальна кіберзагроза критичній інфраструктурі України. За даними експертів Міжнародного валютного фонду, економічні втрати від атаки вірусу «Petya» становили майже 850 млн доларів [4].

Враховуючі означене, вимоги нормативних актів у сфері національної безпеки [5] та спираючись на думки науковців можемо виокремити основні види загроз безпеці у сфері критичної інфраструктури:

- комп'ютерна злочинність;
- інформаційний тероризм;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати громадською думкою, зокрема шляхом поширення недостовірної, неповної або упередженої інформації;
- прояви обмеження свободи слова і доступу громадян до інформації та інших їхніх прав і свобод;
- поширення ЗМІ культу насильства, жорстокості, порнографії та інших проявів аморальності;
- поширення ідеологій та впливу деструктивних неокультів;
- небезпечне для економічної незалежності України зростання частки іноземного капіталу у стратегічних галузях економіки, пов'язаних з інформаційною сферою;
- інспірування інших деструктивних процесів в інформаційній сфері нашої держави.

Означені загрози трансформуються у конкретні злочини, що визначають особливості методики попередження, виявлення їх окремих видів.

В той же час системно історичний підхід до вивчення феномену кримінальної кеіберпротивності свідчить, що звичайний управлінський підхід до протидії кримінальний кіберпротиправності не може бути ефективним.

Адекватність організаційних, спеціальних та процесуальних заходів кіберзагрозам повинна будуватися на синергетичному підході.

Якщо вивчити міжнародний та національний досвід протидії кримінальній кіберпротиправності, то можемо констатувати, що сьогодні не враховується значна кількість чинників, що впливає на формування оптимальної системи протидії загрозам у кіберсфері.

В останні роки методами синергетики було здійснено моделювання таких складних самоорганізуючих систем як формування громадської думки і демографічних процесів. Означений досвід необхідно використовувати при реструктуризації системи протидії кіберзагрозам у сфері критичної інфраструктури.

Але якщо більшість систем Всесвіту носить відкритий характер, то це означає, що у Всесвіті домінують не стабільність і рівновага, а нестійкість і нестабільність. Нестабільні системи мають здатність сприймати відмінності в зовнішньому середовищі і враховувати їх в своєму функціонуванні. Так, деякі слабкіші дії можуть робити більший вплив на еволюцію системи, чим дії, хоч і сильніші, але не адекватніші власним тенденціям системи [6].

Таким чином , можемо зробити висновок , що кіберзлочини – є досить небезпечними кримінальними правопорушеннями, що потребує удосконалення не тільки кримінального законодавства а й формування відповідної моделі моніторингу ситуації загроз у кіберпросторі.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України: Указ Президента України від 25 лютого 2017 року № 47/2017.

2. Аналітичний звіт щодо аналізу гібридних загроз у секторі громадської безпеки та цивільного захисту. Державний науково-дослідний інститут МВС України. Київ. 2019. 13 с.

3. Газізова Ю. Ера цифрових технологій – ера нових злочинів. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «ПРАВО»*. Випуск 29, 2020. URL:/https://uz.ligazakon.ua/ ua/magazine_article/EA013606

4. Веселова Л. Ю. Кібернетичні загрози у контексті сучасного сприйняття їх в Україні/ *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «ПРАВО»*. Випуск 29, 2020. DOI: https://doi.org/ 10.26565/2075-1834-2020-29-22 URL: https://periodicals.karazin. ua/law/article /view/15443

5. Загрози національній безпеці держави в інформаційній сфері. URL : https://pidruchniki.com/1834071936975/politologiya/zagrozi natsionalniy_bezpetsi_ derzhavi_ informatsiyniy_sferi

6. Шинкаренко І.Р. Синергетика та її значення у формуванні оперативно-розшукової політики та стратегії: теоретично-прикладні проблеми. *Сучасні проблеми теорії та практики оперативно-розшукової діяльності органів внутрішніх справ: Матеріали міжнародної науково-практичної конференції 3 червня 2011 р. Запоріжжя.* Запоріжжя: Юридичний інститут ДДУВС, 2011. 206с. С. 185-188.